

# PRBIT - Princípy bezpečnosti informačných technológií

## Report - Domáca úloha č.7

Autor: Marek Čederle

Cvičenie: Pondelok 17:00

### Použité príkazy a ich vysvetlenie

#### Zadanie č.1

1. Na pridelenom virtuálnom PC – Windows Server sa prihláste poskytnutými údajmi do účtu Administrator.
2. \*Vytvorte nový používateľský účet user1, ktorý bude pre bežného používateľa, heslo nastavte „Heslo123456“. Používateľ musí byť členom skupiny Users.  
Dokumentujte výpisom príkazov, z ktorých bude zrejmé, akí používatelia sú na Windows zariadení a akých skupín sú členmi.
3. Prihláste sa novým kontom user1 na server. Je prihlásenie povolené? Ak nie, prečo?
4. \*Nastavte konto user1 do príslušných používateľských skupín tak, aby sa mohol daný používateľ prihlásiť interaktívne na server – v našom prípade postačuje cez vzdialenú pracovnú plochu.
  - a. Dokumentujte snímku obrazovky tak , aby bolo zrejmé, že používateľ user1 je prihlásený.
  - b. Dokumentujte výpisom príkazov, ktoré zobrazia, akých skupín je používateľ user1 členom

2.

```
net user user1 Heslo123456 /add
```

Do skupiny `Users` je automaticky pridaný a vieme to overiť príkazom `net users user1` .

```
# PS C:\Users\Administrator> net users user1
User name                user1
Full Name
Comment
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never

Password last set        28. 10. 2024 17:28:19
Password expires         9. 12. 2024 17:28:19
Password changeable      28. 10. 2024 17:28:19
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               Never

Logon hours allowed      All

Local Group Memberships  *Users
Global Group memberships *None
The command completed successfully.
```

Všetkých užívateľov môžeme zobraziť príkazom `net users`.

```
User accounts for \\WIN-STUDENT-6
```

```
-----
Admin                Administrator      cloudbase-init
DefaultAccount       Guest             user1
WDAGUtilityAccount
The command completed successfully.
```

Ak chceme zistiť skupinu každého používateľa, vieme použiť príkaz, ktorý bol spomenutý vyššie ale nahradíme `user1` za iné používateľské meno.

3.

Nie, pretože na to nemá oprávnenie.

## Pripojenie vzdialenej pracovnej plochy



Pripojenie bolo odmietnuté, pretože používateľské konto nemá oprávnenie na vzdialené prihlásenie.



Skryť podrobnosti

OK

Kód chyby: 0x3

Rozšírený kód chyby: 0x9

Časová pečiatka (UTC): 10/28/24 04:36:01 PM

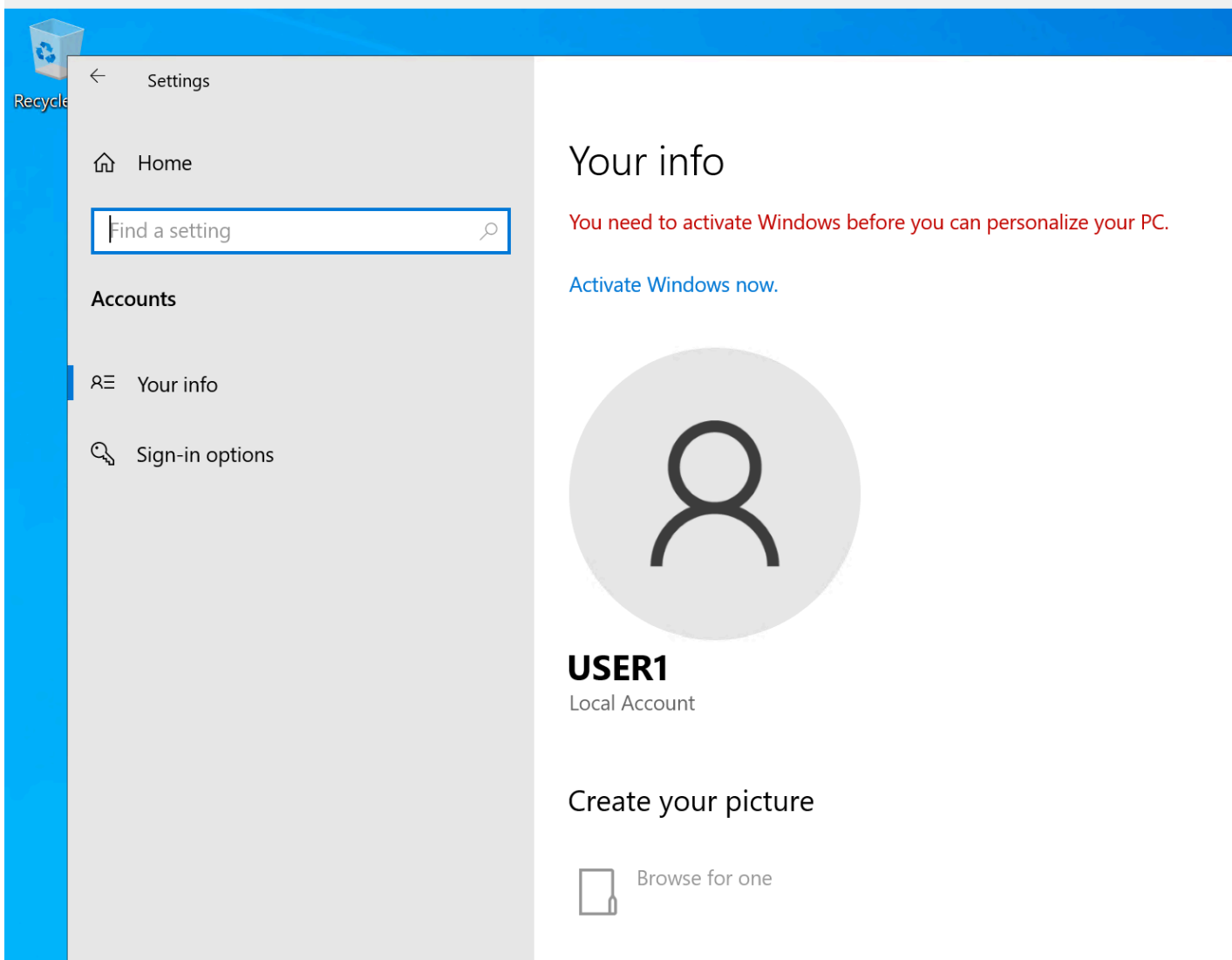
Skopírujte stlačením Ctrl+C.

4.

Keď sa prihlásime znova ako administrátor, môžeme pridať používateľa do skupiny Remote Desktop Users príkazom:

```
net localgroup "Remote Desktop Users" user1 /add
```

- a)



- b)

```

PS C:\Users\Administrator> net localgroup "Remote Desktop Users" user1 /add
The command completed successfully.

PS C:\Users\Administrator> net user user1
User name                user1
Full Name
Comment
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never

Password last set        28. 10. 2024 17:28:19
Password expires         9. 12. 2024 17:28:19
Password changeable      28. 10. 2024 17:28:19
Password required        Yes
User may change password  Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               28. 10. 2024 17:36:02

Logon hours allowed      All

Local Group Memberships  *Remote Desktop Users *Users
Global Group memberships *None
The command completed successfully.

```

## Zadanie č.2

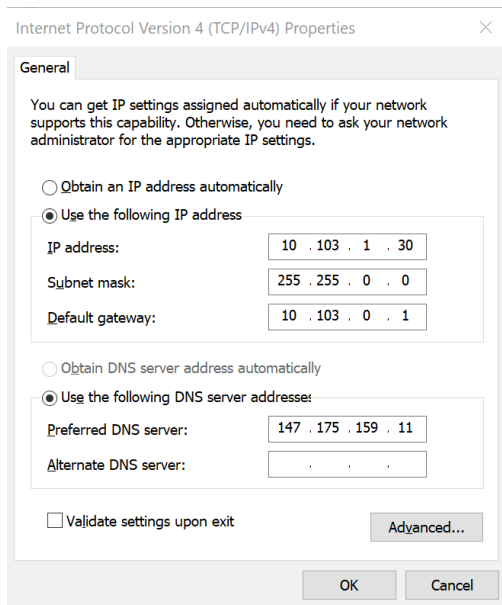
Vašou úlohou je zriadiť doménu Active Directory a „povýšiť“ Váš Windows server na radič domény/doménový kontrolór ADDC.

- Premenujte Váš server – zmeníte mu hostname na ADDC (dobrá prax, po vytvorení domény je zmena názvu hostname komplikovanejšia)
- Nastavte statickú IP adresu Vášmu serveru – zobrazte si aktuálne parametre siete a nastavte ich staticky – pretože nedá sa zriadiť doménový radič tak, aby mal IP adresu z DHCP (pretože na ADDC je súčasťou adresárovej služby aj DNS server)
- Nainštalujte rolu Active Directory Domain Services a DNS server.
- Povýšte Váš server na doménový radič a vytvorte novú doménu „vasemeno.local“, pričom za vasemeno **je nutné dosadiť Vaše krstné meno**. Riešenia s iným názvom domény než je Vaše krstné meno nebudú akceptované!
- Server sa na záver reštartuje. Prihláste sa naň.

- Zmena mena na ADDC



- Nastavenie statickej IP adresy



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> ipconfig /all

Windows IP Configuration

Host Name . . . . . : ADDC-xcederlem
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : openstacklocal

Ethernet adapter tap2d36ad6-05:

Connection-specific DNS Suffix . : openstacklocal
Description . . . . . : Red Hat VirtIO Ethernet Adapter
Physical Address. . . . . : FA-F1-17-8C-44-13
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::d1b0:ed7d:c1ed:6831%7(Preferred)
IPv4 Address. . . . . : 10.103.1.30(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Lease Obtained. . . . . : pondelok 28. októbra 2024 18:01:39
Lease Expires . . . . . : utorok 29. októbra 2024 18:01:39
Default Gateway . . . . . : 10.103.0.1
DHCP Server . . . . . : 10.103.1.3
DHCPv6 IAID . . . . . : 284881175
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-A5-50-85-52-54-00-E3-A1-96
DNS Servers . . . . . : 147.175.159.11
NetBIOS over Tcpip. . . . . : Enabled

PS C:\Users\Administrator>
```

- Nainštalovanie Active Directory a DNS servera

Add Roles and Features Wizard

DESTINATION SERVER  
ADDG-xcederlem

Select server roles

Before You Begin

Installation Type

Server Selection

**Server Roles**

Features

AD DS

DNS Server

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

☐ Active Directory Certificate Services

☒ Active Directory Domain Services

☐ Active Directory Federation Services

☐ Active Directory Lightweight Directory Services

☐ Active Directory Rights Management Services

☐ Device Health Attestation

☐ DHCP Server

☒ DNS Server

☐ Fax Server

☒ File and Storage Services (1 of 12 installed)

☐ Host Guardian Service

☐ Hyper-V

☐ Network Policy and Access Services

☐ Print and Document Services

☐ Remote Access

☐ Remote Desktop Services

☐ Volume Activation Services

☐ Web Server (IIS)

☐ Windows Deployment Services

☐ Windows Server Update Services

Description

Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.

< Previous

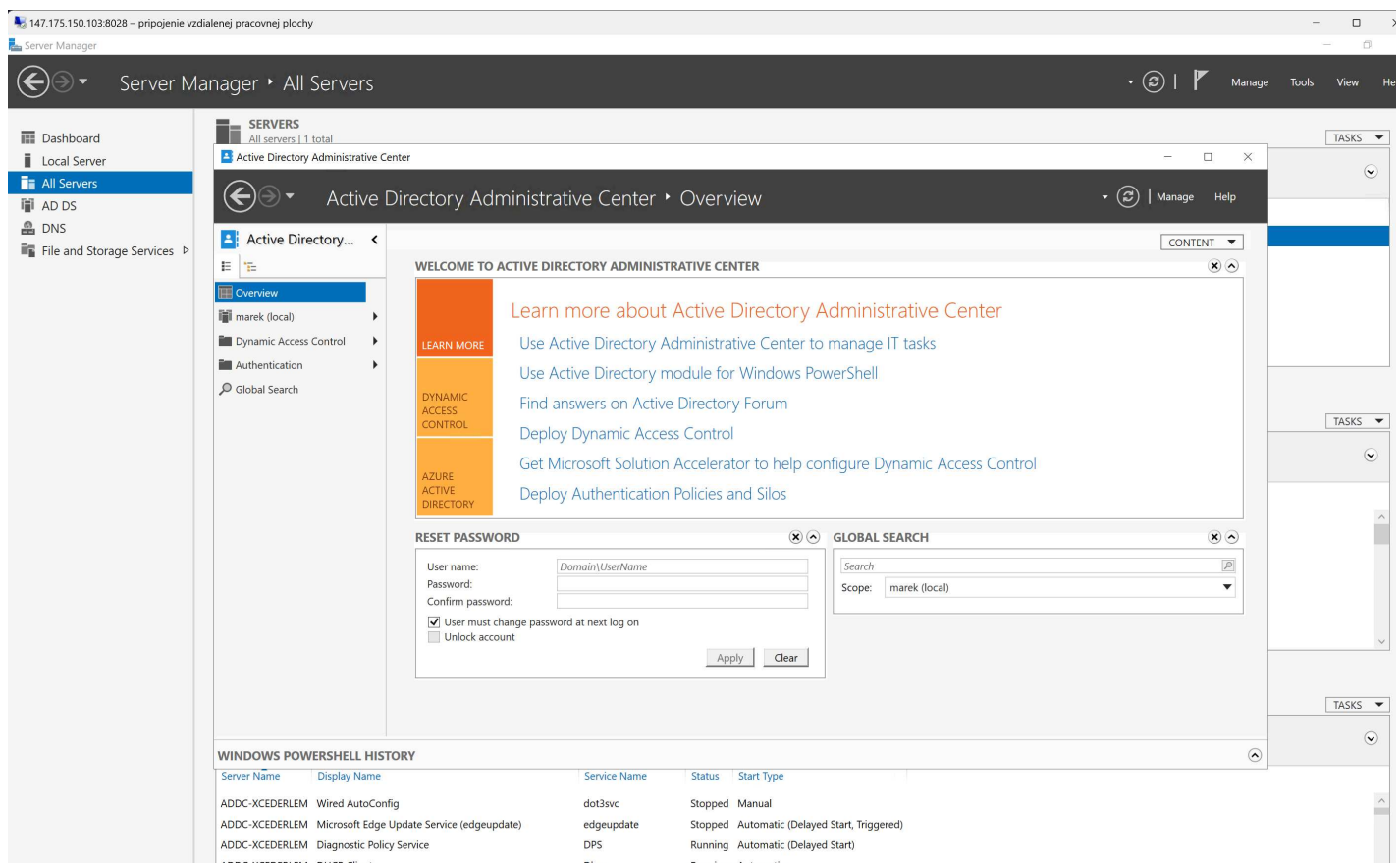
Next >

Install

Cancel

- Úspěšně nainstalovaný DNS a AD radič





### Zadanie č.3

## Úloha 3 - vytvorenie štruktúry domény a používateľa

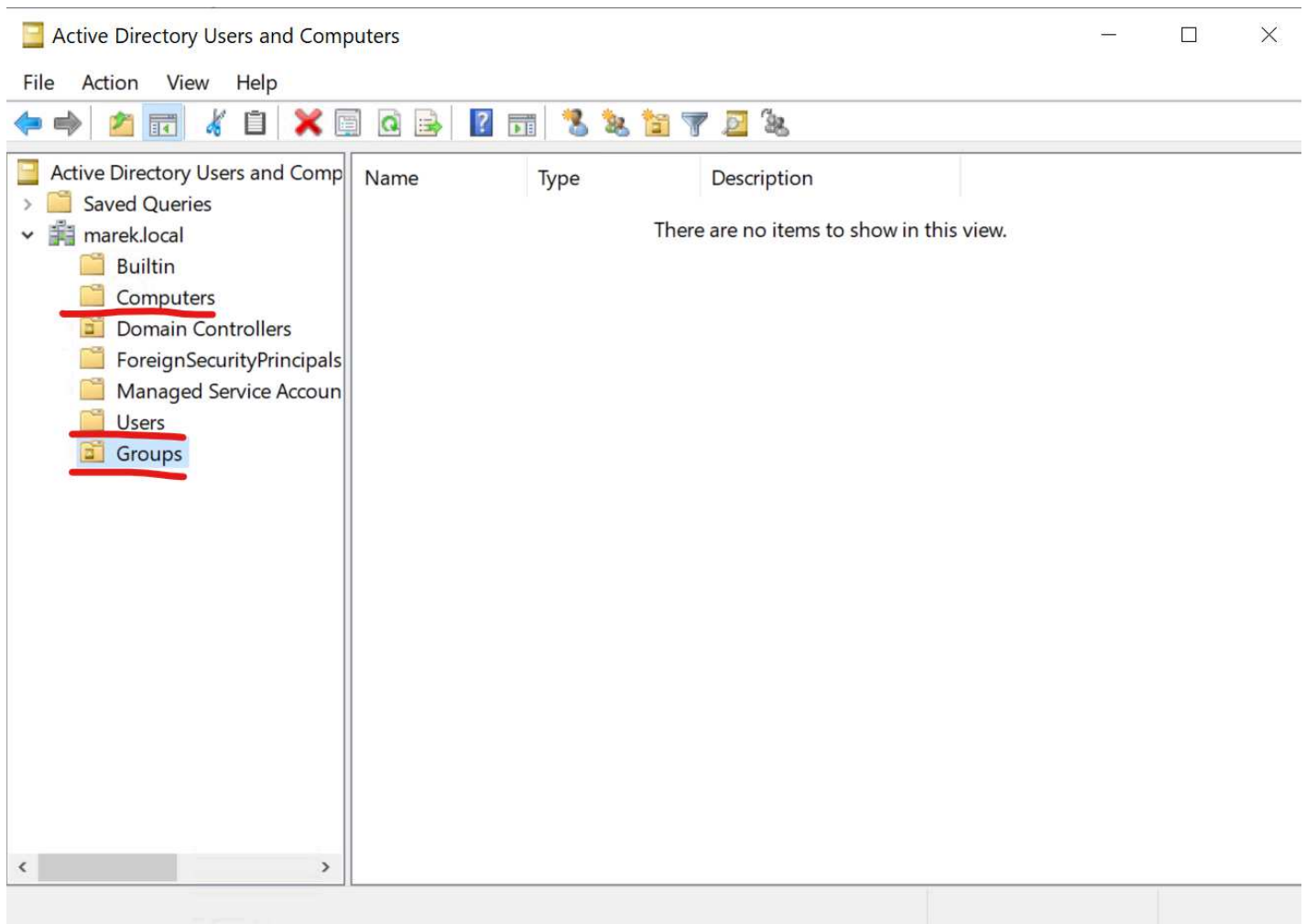
Hodnotenie: 1 b

Svoj postup dokumentujte snímkami obrazovky a stručnými komentármi.

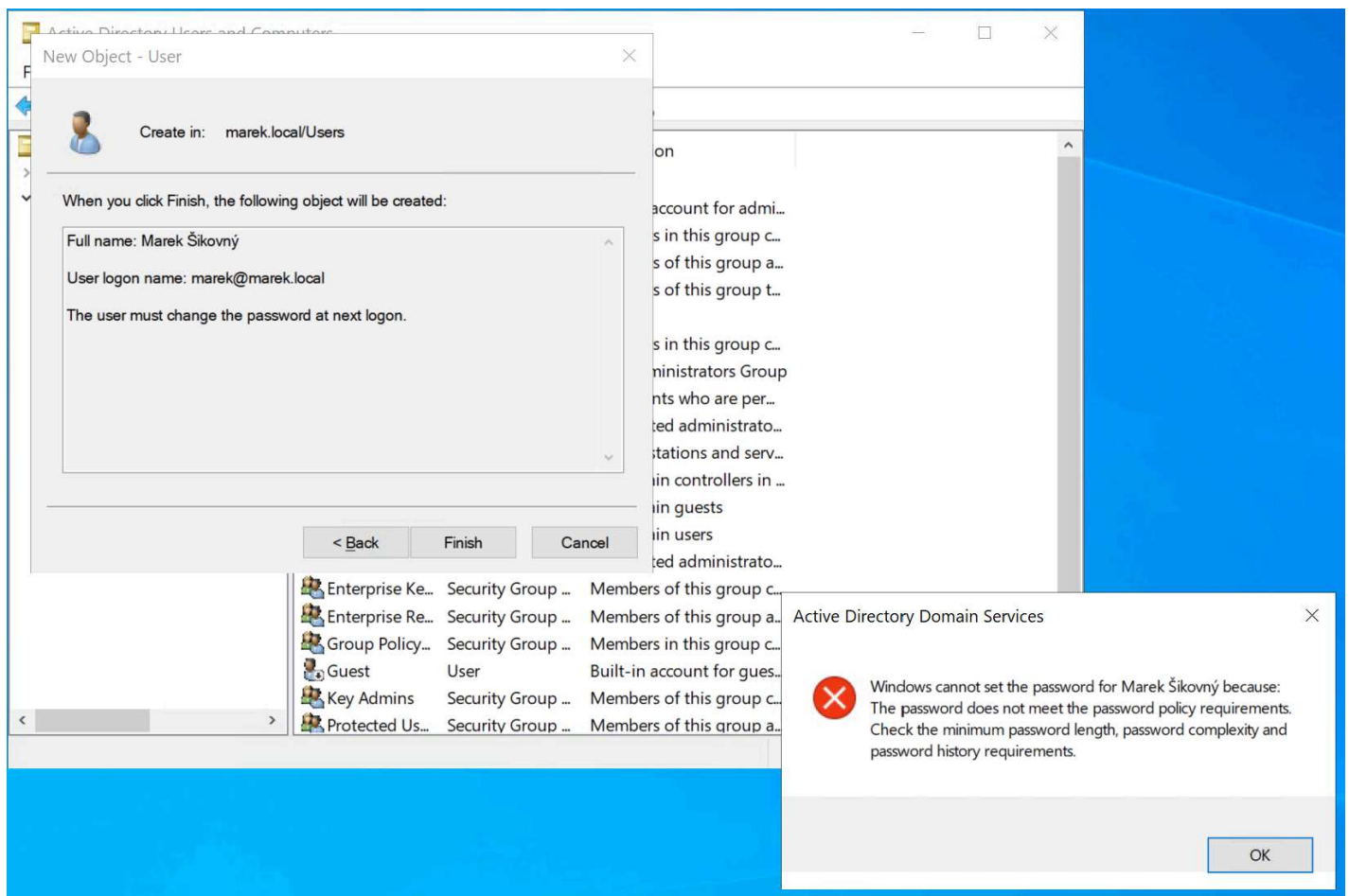
- Pomocou na to určených nástrojov (GUI či PowerShell moduly) vytvorte organizačnú štruktúru domény. Predovšetkým vytvorte organizačné jednotky pre používateľov, počítače a skupiny.
- Do organizačnej jednotky pridajte používateľa, ktorý bude mať login name Vaše krstné meno, meno – Vaše krstné meno, priezvisko – Šikovný. **Riešenia s iným menom než je Vaše krstné meno nebudú akceptované!**  
Heslo nastavte abc
- Systém Vám oznámi, že takéto heslo nie je možné akceptovať. Zistite, aká je aktuálne platná politika hesla na Vašom serveri a podľa toho vytvorte vlastné heslo, ktoré uvediete do riešenia, spolu so znením príslušnej politiky hesla. **Upozornenie – na každom z Windows Serverov je nastavená iná politika hesla.**  
Politiku hesla je možné zistiť rôznymi spôsobmi, pričom preferujeme v tomto prípade postup jej zistenia pomocou GUI. Pomôcka – pomocou GUI nenájdete nástroj „password policy“, také vo Windows neexistuje, ale tieto opatrenia sú špecifikované v rámci „celého balíka“ opatrení.

- Organizačné jednotky `Users` a `Computers` boli už vytvorené, takže som vytvoril už iba OU `Groups`.

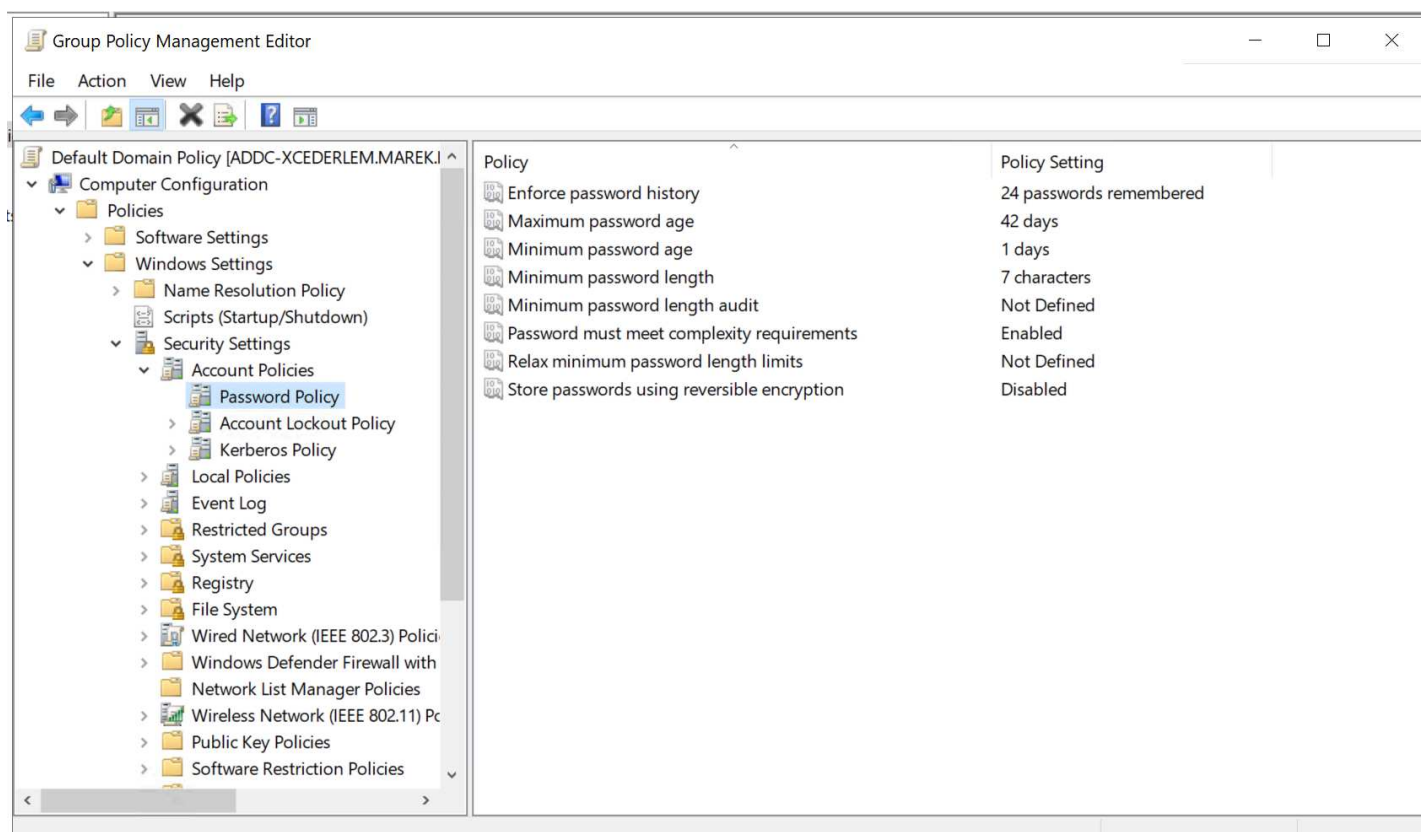




- Vytvorenie používateľa



- Zistenie politík pre tvorbu hesla



- Heslo: `xceder1em123*` Toto heslo spĺňa všetky požiadavky, ktoré sú nastavené v politike pre heslá.

1. Prostredníctvom skupinovej politiky nastavte odporúčané nastavenia Politiky hesla a zamykanie účtov. Riešenie je potrebné realizovať **vytvorením vlastného objektu skupinovej politiky tak, že samotný objekt skupinovej politiky sa musí volať „Politika hesla – VaseKrstneMeno“**. Riešenia s politikou v názve neobsahujúcou Vaše krstné meno nebudú akceptované.

Študijný materiál: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy>

Nastavte:

- platnosť hesla jeden rok
- minimálny vek hesla nedefinujte – resp. nastavte aby nebol vyžadovaný
- dĺžka hesla 10 znakov
- komplexita hesla – povoľte + stručne jednou vetou vysvetlite, aké znaky musí obsahovať heslo aby bolo v prostredí MS Windows považované za komplexné
- nastavte zamknutie konta pri neúspešnom prihlasovaní nasledovne:

Account Policies/ Account Lockout Policy	
Policy	Setting
Account lockout duration	35 minutes
Account lockout threshold	7 invalid logon attempts
Reset account lockout counter after	35 minutes

2. Zistite, aký príkaz je potrebné použiť na to, aby sa zadefinované možnosti v politike aplikovali, prípadne zdôvodnite, či je potrebné reštartovať server.
3. Zdôvodnite, prečo je dôležité, aby bola stanovená Minimum password age, môžete ilustrovať na príklade. Nápoveda – berte do úvahy, že v podnikovom prostredí je heslo používateľa synchronizované pomocou adresárovej služby LDAP a používa sa na prihlásenie sa k Office365, AIS, interné informačné systémy, VPN, ...
4. Prostredníctvom printscreenov ukážte, kde je možné nastaviť v skupinovej politike voľbu vynútenia stlačenia kombinácie kláves CTRL+ALT+DEL pri prihlasovaní sa do PC. Zároveň vysvetlite, prečo je vhodné toto nastavenie povoliť.

Group Policy Management Editor

File Action View Help

Politika hesla - Marek [ADDC-XCEDERLEM.MAREK.LOCAL] Policy

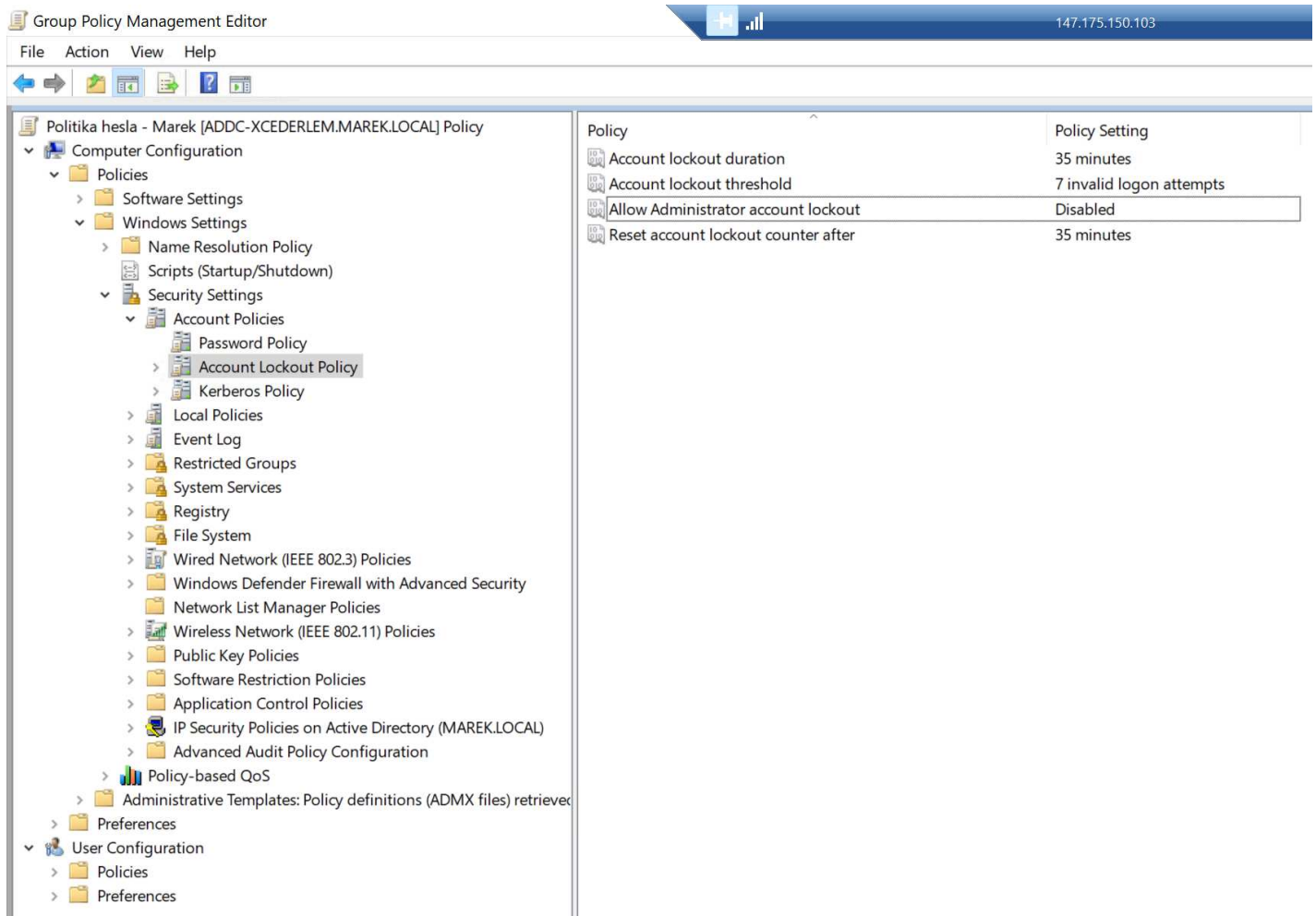
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
          - Password Policy**
            - Account Lockout Policy
            - Kerberos Policy
            - Local Policies
            - Event Log
            - Restricted Groups
            - System Services
            - Registry
            - File System
            - Wired Network (IEEE 802.3) Policies
            - Windows Defender Firewall with Advanced Security
            - Network List Manager Policies
            - Wireless Network (IEEE 802.11) Policies
            - Public Key Policies
            - Software Restriction Policies
            - Application Control Policies
            - IP Security Policies on Active Directory (MAREK.LOCAL)
            - Advanced Audit Policy Configuration
          - Policy-based QoS
          - Administrative Templates: Policy definitions (ADMX files) retrieved
        - Preferences
  - User Configuration
    - Policies
    - Preferences

Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	365 days
Minimum password age	0 days
Minimum password length	10 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Not Defined

Komplexné heslo musí spĺňať nasledujúce požiadavky:

- nesmie obsahovať meno používateľa alebo časti celého mena používateľa, ktoré presahujú dva po sebe idúce znaky
- mať dĺžku aspoň 6 znakov
- obsahovať znaky aspoň z troch z nasledujúcich štyroch kategórií:
- veľké anglické znaky (A až Z)
- a nglické malé písmená (a až z)
- číslice (0 až 9)
- nealfabetické znaky (napríklad !, \$, #, %) (špeciálne znaky)

Nastavenie pre zamknutie účtu:



2.

```
gpupdate /force
```

Príkaz spustí vynútenú aktualizáciu politík skupiny a aplikuje všetky politiky bez čakania na ďalšie plánované obnovenie.

V tomto prípade nie je treba reštartovať server, ale ak nám toto zlyhá z nejakého dôvodu (napr. nedostatočné oprávnenia a pod.), tak je vhodné reštartovať server.

3.

Bez `Minimal password age` by používatelia mohli rýchlo zmeniť svoje heslo niekoľkokrát za sebou, aby sa vrátili k pôvodnému heslu. Napríklad, ak je politika hesla nastavená tak, že heslo môže byť rovnaké až po 5 zmenách (t.z. pamäť si históriu hesiel), bez tejto politiky by používateľ by mohol zmeniť heslo 5-krát za sebou a vrátiť sa k pôvodnému heslu, čím by vedel obísť tieto bezpečnostné opatrenia. Ďalším dôvodom je, že v podnikovom prostredí, kde sa heslá nejako synchronizujú a používajú sa na prihlásenie do rôznych systémov, tak je dôležité, aby heslá zostali konzistentné po nejakú určitú dobu pretože by mohlo dôjsť ku nejakým problémom, že niekde by bolo heslo zmenené a niekde nie a nevedel by sa používateľ prihlásiť na danú službu.

4.



Group Policy Management Editor

File Action View Help

147.175.150

Politika hesla - Marek [ADDC-XCEDERLEM.MAREK.LOCA]

- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Policies
        - Windows Defender Firewall with Adv...
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11) Policie
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Active Director
        - Advanced Audit Policy Configuration
      - Policy-based QoS
      - Administrative Templates: Policy definitions
    - Preferences
  - User Configuration
    - Policies
    - Preferences

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to cons...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vista...	Not Defined
Audit: Shut down system immediately if unable to log securit...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor Def...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor De...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user on...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow computer account re-use during do...	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure channel...	Not Defined
Domain controller: LDAP server channel binding token requir...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel dat...	Not Defined
Domain member: Digitally encrypt secure channel data (when...	Not Defined
Domain member: Digitally sign secure channel data (when po...	Not Defined
Domain member: Disable machine account password changes	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) sess...	Not Defined
Interactive logon: Display user information when the session ...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Not Defined
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in cas...	Not Defined
Interactive logon: Prompt user to change password before ex...	Not Defined
Interactive logon: Require Domain Controller authentication t...	Not Defined
Interactive logon: Require Windows Hello for Business or sma...	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Microsoft network client: Digitally sign communications (alwa...	Not Defined
Microsoft network client: Digitally sign communications (if se...	Not Defined
Microsoft network client: Send unencrypted password to thir...	Not Defined

Skratka **CTRL+ALT+DEL** je kombinácia kláves, ktorá je určená pre systém a iba ten ju vie zachytiť. To znamená, že v prípade ak by na našom počítači bol nejaký malware, tak by nemohol zachytiť túto kombináciu klávesov (napr. nejaká phishing obrazovka, ktorá by sa tvárila ako daná obrazovka na zadávanie hesla), čo pre používateľa vzbuduje dôveru v daný systém a tvorí bezpečné prostredie.